



FTK Asia™

FTK Asia is AccessData's latest product for the forensic analysis market. FTK Asia supports Unicode text, file filtering and identification, indexing and search functionality.[†]

Feature Set:

Unicode Support

The most distinguishing feature of FTK Asia is its ability to read, search, and utilize Unicode characters. This makes FTK Asia the exclusive solution for investigations involving digital evidence from Asian regions, or any other region that uses non-ANSI characters. FTK Asia supports both UTF-8 and UTF-16LE formats.

Multiple Evidence Sources

There are four specific types of evidence that FTK Asia has the ability to read and process into cases; physical drives, logical drives, over 25 different image file types, and the contents of any folder local to the analyzing computer.

Drive Imaging

Any type of hard or swappable drive can be imaged, preserved and saved as single or multiple files by FTK Asia. This allows an investigator to make an exact copy of a suspect drive, preserving its original state so that any evidence obtained cannot be altered or manipulated in any way. All investigation of evidence will be performed on the image of the suspect drive.

Hashing

When a physical or logical device is imaged, hashes are automatically computed in both the MD5 (Message-Digest, 64 bit) and SHA1 (Secure Hash Algorithm, 80 bit) formats. These can be used to ensure that the image has not been altered in any way. Hashes may also be computed for files that have been added as evidence.

Word Lists

If the investigation requires the decryption of password protected files, FTK Asia can create a word list which will contain every word that appears in the clear on a suspect drive. This permits the investigator to import this list as a "dictionary" into a tool such as the Password Recovery Toolkit (PRTK) to assist in the cracking of a user's password.

Report Generation

FTK Asia produces an XML report detailing all of the items that were bookmarked during the investigation process. A simple XSL style sheet is provided to present this information in a clear and readable manner. Of course the style sheet can be customized to reflect your particular needs as you desire.

Multiple Evidence Views

FTK Asia offers four different views for inspecting evidence, these include Automatic View (through Internet Explorer), Filtered View (using the Content Access filtering software), Plain Text (ANSI), and Hex View (for binary display).

Indexed and Live Search

It is often necessary to search for particular text strings that are pertinent to a case. In order to provide the investigator with the tools to adequately recover such specific evidence, FTK Asia provides the ability to perform both Live and Indexed searches.

Live search will allow an investigator to search the entire image for the selected search string (in UTF-8, UTF16LE or binary form) from beginning to end. This is the most thorough, but time consuming, search. If desired, the data may be filtered with Content Access to provide a translation to UTF-16LE as the search is performed.

Indexed search is only available after all or part of the image has been indexed, which is done after the files have been filtered with Content Access and converted to UTF-16LE format. Word breaks are done on a space/symbol basis, therefore for most non-ANSI searches it may be necessary to surround the search term with wild card ('*') characters.

Data Carving

One of the most important evidence recovery features offered by FTK Asia is its ability to "carve" for specific data from all parts of a drive. This option will allow an investigator to recover files such as hidden graphics, text, spreadsheets, and PDF files. These types of carved files may reside in previously deleted files, within drive slack or unallocated space, or embedded within other file formats.

Bookmarking

With the ability to bookmark recovered evidence, the investigator has an easy way of tagging and setting aside any items that may be pertinent to the case being investigated. Any file within the image can be bookmarked, which will automatically add that item to the "Bookmarks" file list, enabling quick recovery at any time. Bookmarked items are included in the generated case report.

Hex Value Interpreter

When an investigator is analyzing evidence displayed within the Hex View of FTK Asia, they will have the ability to quickly assess digital evidence (such as time stamps) by utilizing FTK Asia's Hex Value Interpreter.

Multiple Evidence Handling

FTK Asia has the ability to add as many evidence items as necessary to a case. These evidence items would include any of the evidence sources mentioned previously. It is also possible to remove evidence items from a case if it is concluded that they are no longer necessary or relevant to other evidence items within a case.

Movable Panels

Every panel, within FTK Asia can be undocked and moved to another location, either within the main FTK Asia window or outside, as a standalone window.

Logicube Support

Forensic Docks, made by Logicube, can be used seamlessly from within FTK Asia through an investigator's parallel and USB ports. Suspect drives may be copied using FTK Asia's imaging abilities, with the added protection of Logicube's Forensic Dock write protection capabilities.

Usage Recommendations:

1. Update Internet Explorer

In order to avoid unexpected errors originating from the file viewer, it is necessary to update Internet Explorer to the latest version available, it is recommended to be current up to at least IE version 6.

2. Carving an Entire Image

The investigator has the option in FTK Asia to either carve individual parts or all parts of the image at the same time. The best way to carve the entire image is outlined in the following steps:

- a. Select the root of the Evidence Tree (the image name)
- b. Select the File List pane
- c. Select all files listed in the File List pane
- d. Right-click the selected files and choose the "Carve for Files" option

3. Carved Items Folder

The carved items folder is not included in any of the recursive operations performed on the root of the evidence. Any operations that need to be done on the items in this folder (such as a count of files in a particular category) must be performed as a separate step after selecting the Carved Items folder explicitly.

4. Hashing

File hashes are computed manually, not automatically. If it is necessary to obtain a file's hash value, it may be acquired by selecting the file, or files, and then right-clicking and selecting "Export File Hash List." The hash values will be exported into a tab-delimited MS Excel .csv file. The computed values will be added to the case.

5. Index Search

If search hits are returned in files that are particularly large (about 100 MB or more) Internet Explorer will take an extraordinarily long time to load this file after it has been converted to HTML for display purposes. Therefore the delay after clicking on a hit and the display of the hit can be considerable.



User Manual Errata:

1. "Exporting File Hash Lists" (pg. 54)

After step 5, it is mentioned that hash lists are saved as a file of comma-separated values in a .csv file type. Although it is true that hash lists are in fact saved in a .csv file, the values are not comma-separated, they are actually tab-separated in order to be displayed properly in MS Excel.

2. Appendix A (pg. 99)

This appendix consists of file types that should be recognized by FTK Asia when performing a forensic analysis. At the moment however, contrary to what is shown in this list, FTK Asia does not recognize the following file types: AOL e-mail, AOL instant messaging files, AOL/AIM Buddy lists, and Thumb.db archives.

3. System Requirements

Minimum Requirements

OS ----- Windows 2000
Processor ----- Intel Pentium III or AMD Athlon
RAM ----- 512 MB
Monitor ----- SVGA (800 x 600)
Hard Disk space ----- 30 MB
Dongle Support ----- USB or Parallel Port

Recommended Requirements

OS ----- Windows XP
Processor ----- Intel Pentium 4, AMD Athlon XP, or higher
RAM ----- 1 GB or higher
Monitor ----- XGA (1024 x 768) or higher

[†]Note to FTK 1.x Users:

FTK Asia has many similarities to the original AccessData Forensic Toolkit, but it does not have the same feature set. Do not expect to be able to do the same things with FTK Asia that you can do with FTK 1.x. FTK Asia's primary purpose is to provide a means to forensically analyze non-ANSI systems. Therefore, FTK 1.x will not always provide the same results as FTK Asia.